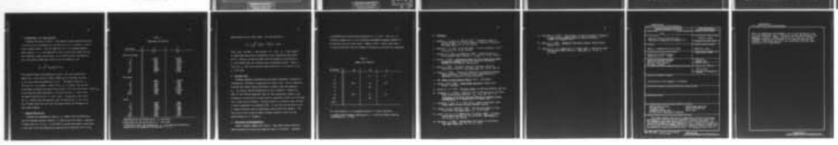
AD-A046 149 NORTH CAROLINA UNIV AT CHAPEL HILL F/G 9/2
EMPIRICAL TESTING OF MULTIPLICATIVE CONGRUENTIAL GENERATORS WIT--ETC(U)
OCT 77 G S FISHMAN, L R MOORE N00014-76-C-0302
UNCLASSIFIED TR-77-12 NL

1 OF 1
AD
A046149



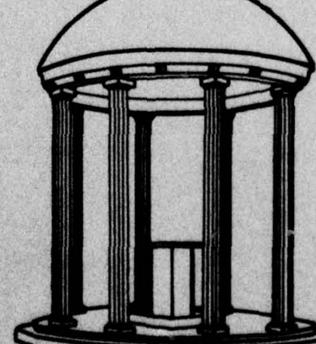
END
DATE
FILMED
12-77
DDC

12

B.S.

OPERATIONS RESEARCH AND SYSTEMS ANALYSIS

UNIVERSITY OF NORTH CAROLINA
AT CHAPEL HILL



6

EMPIRICAL TESTING OF MULTIPLICATIVE CONGRUENTIAL GENERATORS WITH MODULUS $2^{31}-1$

10 George S. Fishman [redacted] Louis R. Moore

9 Technical Rep[redacted]t 77-12

11 Oct[redacted]77

12 20p.

14 TR-77-12

15 N00014-76-C-0302

Curriculum in Operations Research
and Systems Analysis

University of North Carolina at Chapel Hill

259 500

This research was supported by the Office of Naval Research under contract N00014-76-C-0302. Reproduction in whole or in part is permitted for any purpose of the United States Government.

2 TO THE 31st POWER

-Ø-

ABSTRACT

This paper presents the results of empirically testing 8 alternative multipliers for a multiplicative congruential generator with modulus $2^{31}-1$. The LLRANDOM random number package ~~[11]~~ uses one of the multipliers, the simulation programming language SIMSCRIPT II uses a second and the remaining six are the best of 50 candidate multipliers studied by Hoaglin (1976) using the theoretical spectral and lattice tests. The battery of tests fail to detect any departures from randomness for 3 of the multipliers, even at a 0.20 significance level. This group includes the multiplier that SIMSCRIPT II employs. However, another of the 3 superior performers, 397204094, requires only 78 percent of the computing time that the SIMSCRIPT II multiplier does and is the second most efficient computationally of all 8 multipliers.

1. Introduction

This paper presents the results of empirically testing 8 multipliers suggested in the literature for use in a multiplicative congruential pseudo-random number generator with modulus $2^{31}-1$. Generators of this type are in common use, although Marsaglia (1968) has shown that all such congruential generators, whether they be of modulus 2^{β} or of prime modulus, possess flaws that make their theoretical properties differ from those of an ideal source of random numbers. Since these departures from ideal properties conceivably could cause serious errors in practice, submitting these generators to empirical testing provides a way of evaluating their performance.

Consider the linear congruential multiplicative generator

$$(1) \qquad Z_i \equiv AZ_{i-1} \pmod{M}$$

where $M = 2^{31}-1$. In order that (1) generate all integers in $[1, M-1]$ before cycling, A must be a primitive root of M [8]. Although $\{V_i = Z_i/M \;;\; i = 1,\ldots,M-1\}$ denotes a sequence of $2^{31}-2$ distinct fractions in (0,1), with spacing 2^{-31} and each with a finite binary representation, this sequence is not the one encountered in practice. Because of the need to assign a byte to the exponent of a floating point number, a common procedure on IBM 360/370 system computers generates the fractions $\{U_i = (2[Z_i/2^8] + 1)/2^{24} \;;\; i = 1,\ldots,M-1\}$ where $[\theta]$ denotes the integer part of θ†. Then the sequence $\{U_i\}$ has $2^{31}-2$ fractions per cycle

†See Learmonth and Lewis (1969) and Payne, et al. (1969).

that assume 2^{23} values in $[1/2^{24}, 1 - 1/2^{24}]$ in increments of $1/2^{23} = 0.119209... \times 10^{-6}$. Moreover, the fractions $1/2^{24}$ and $1-1/2^{24}$ occur 2^8-1 times per cycle whereas each of the other fractions occurs 2^8 times per cycle, indicating only a minute departure from uniformity. This density of points seems sufficient for most purposes.

Although the density consideration in (0,1) is important, the issue of randomness is paramount. Presumably one would like to choose a multiplier A such that treating $\{U_i\}$ as a sequence of i.i.d. random variables from $U(0,1)$ introduces incidental error. Lewis, et al. (1969) recommend A = 16807 and fail to detect departures from the assumptions of independence and uniformity in their empirical testing. Learmonth and Lewis (1973) use this multiplier in their random number generator LLRANDOM, as do the discrete event simulation programming language SIMPL/1 [7] and APL [9]. Payne, et al. (1969) recommend A = 630360016 and claim that their testing shows no departures from assumptions.

Recently Hoaglin (1976) screened 50 primitive roots of M using the spectral [3] and lattice [15] tests. These theoretical tests provide an indication of the relative desirability of alternative multipliers for generating k-tuples. The present study reports on how the Lewis, et al. choice A = 16807 (multiplier I), the Payne, et al. choice A = 630360016 (multiplier II) and the best 6 (multipliers III through VIII) chosen from Hoaglin's study fare when subjected to identical empirical testing.

2. Testing Procedure

Three hypotheses were tested:

H_1 . $\{U_i\}$ is a sequence of i.i.d. random variables.

H_2 . U_i has a uniform distribution on (0,1).

H_3. $V_i \equiv (U_{2i-1}, U_{2i})$ has a uniform distribution on the unit square.

For each multiplier the data base consisted of $n = 100$ nonoverlapping samples or replications each of $N = 200{,}000$ U_i . For each of the 100 replications and each hypothesis a statistic, whose asymptotic distribution was known, was computed from the 200,000 observations. Then the 100 statistics for a given generator and specific hypothesis were subjected to a battery of goodness-of-fit tests designed to detect departures of their empirical cumulative distribution functions (cdf's) from their corresponding theoretical cdf's.

3. Runs Up and Down Test Statistic

To test H_1 we relied on runs up and down statistics. Let R_i denote the number of runs up and down of length i for $i = 1,\ldots,6$. Then under H_1 the quantity

$$(2) \qquad R = \sum_{i,j=1}^{6} c_{ij}[R_i - E(R_i)][R_j - E(R_j)]$$

asymptotically has the chi-square distribution with 6 degrees of freedom. Here c_{ij} denotes the element in row i and column j of the inverse of the covariance matrix of $R_1,\ldots,R_6$. Levene and Wolfowitz (1944) present expressions for this covariance matrix and for $E(R_i)$. For $N = 200{,}000$ one has $E(R_1) = 83{,}320.63$, $E(R_2) = 36{,}664.49$, $E(R_3) = 10{,}556.38$, $E(R_4) = 2296.15$, $E(R_5) = 411.44$, $E(R_6) = 61.79$ and $E(R_{7+}) = 9.09$. Here R_{7+} denotes the number of runs of length 7 or more. Although a statistic similar to (2) that incorporates R_{7+} can be constructed and asymptotically has a chi-square distribution with 7

degrees of freedom, the small value of $E(R_{7+})$ in the present case encouraged us to work with (2), thereby avoiding any discretization error that inclusion of R_{7+} might induce.

Let the superscript (i) denote the ith replication for a given multiplier. Also let $W^{(i)} = 1 - P(R^{(i)})$ denote a probability integral transformation so that $W^{(i)}$ has the uniform distribution on $(0,1)$. Then

$$F_n(t) = \frac{1}{n} \Sigma_{i=1}^{n} \; I_{(0,t]}(W^{(i)}) \qquad\qquad 0 \le t \le 1 ,$$

where I denotes the indicator function, is an empirical cdf. Figure 1 shows $F_n(t)$ with $n = 100$ for each multiplier and column 1 of Table 1 lists the Kolmogorov-Smirnov statistics $D_n = \sup|F_n(t) - t|$. Notice that the test fails to reject H_1 for each multiplier at the $\alpha = 0.10$ level but rejects multiplier III at the $\alpha = 0.20$ level.

4. Chi-Square Test Statistic

To test H_2 we chose a chi-square goodness-of-fit statistic. Consider K cells on the unit interval each of length $1/K$. Let N_k denote the number of the n observations on a given replication that fall into the interval $((k-1)/K, k/K]$. Then for a specified K

$$C = \frac{K}{N} \Sigma_{k=1}^{K} (N_k - N/K)^2 = \frac{K}{N} \Sigma_{k=1}^{K} N^2{}_k - N$$

asymptotically has a chi-square distribution with $K-1$ degrees of freedom. Choosing $K = 2^{12} = 4096$ implied a cell width $1/K = 0.000244140625$ and enabled

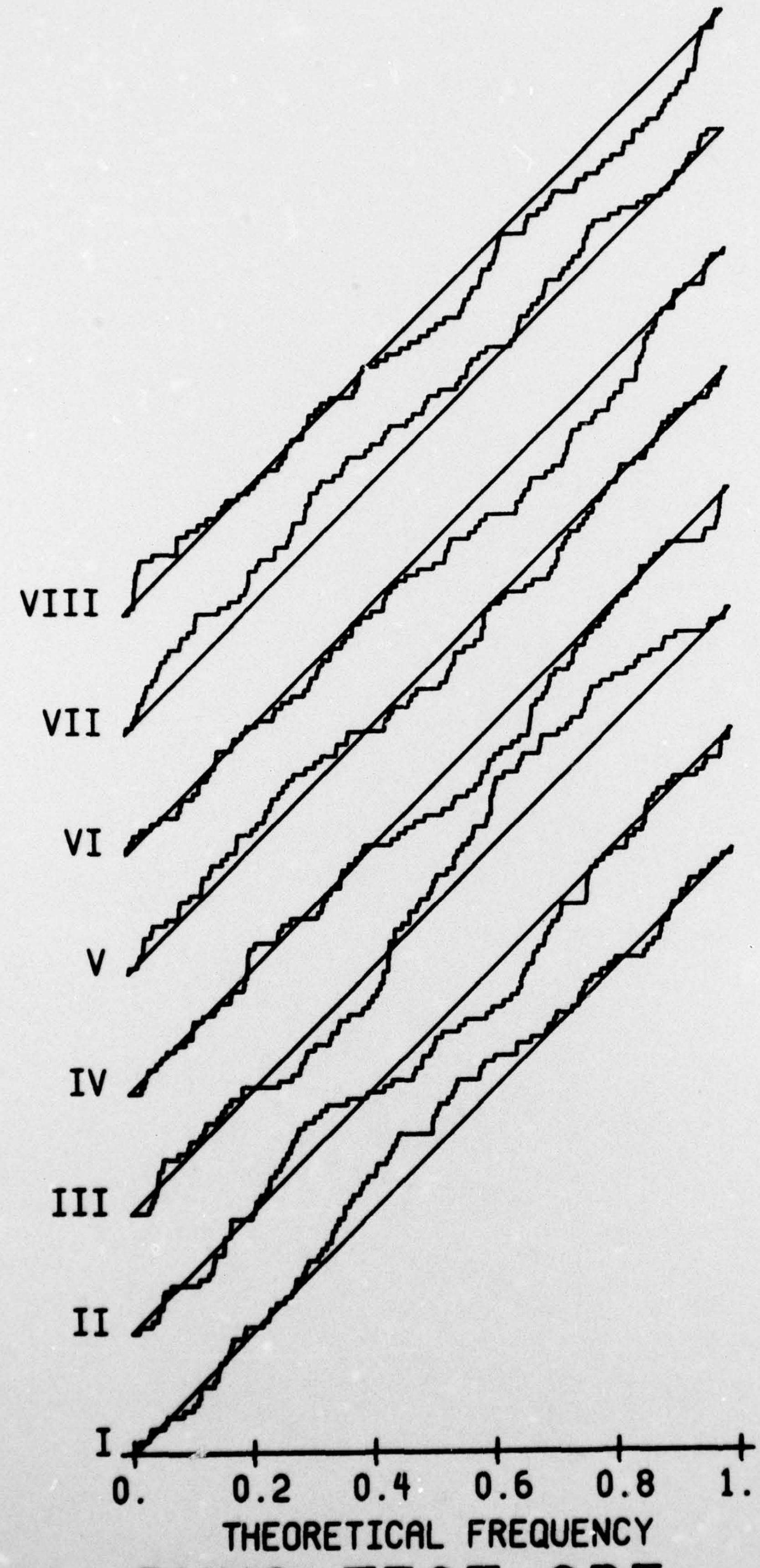


Figure 1. RUNS TEST CDF

us to test the first 12 bits of U_i .

Table 1

Kolmogorov-Smirnov Test Results D_n
$n = 100$

	Multiplier	Runs Up and Down (1)	Chi-Square (2)	Serial (3)	Relative Execution Time (4)
I	16807	0.0856	0.1008	0.0970	1
II	630360016	0.0852	0.0558	0.0884	3.03
III	1078318381	0.1068**	0.0642	0.0850	4.42
IV	1203248318	0.0788	0.0743	0.0816	4.82
V	397204094	0.0542	0.1052	0.0758	2.37
VI	2027812808	0.0919	0.1071**	0.0673	7.28
VII	1323257245	0.0903	0.0926	0.0723	5.31
VIII	764261123	0.0746	0.1033	0.1048	3.46

$\alpha \equiv \Pr(D_{100} > D^*_{100})$, Source: Owen (1962) .

α	D^*
.10	.12067
.20	.10563

Figure 2 shows the empirical cdf's of C for the 8 multipliers and column 2 of Table 1 lists the Kolmogorov-Smirnov statistics. Again, the test fails to reject H_2 for each multiplier at the $\alpha = 0.10$ level; however, it now rejects multiplier VI at $\alpha = 0.20$.

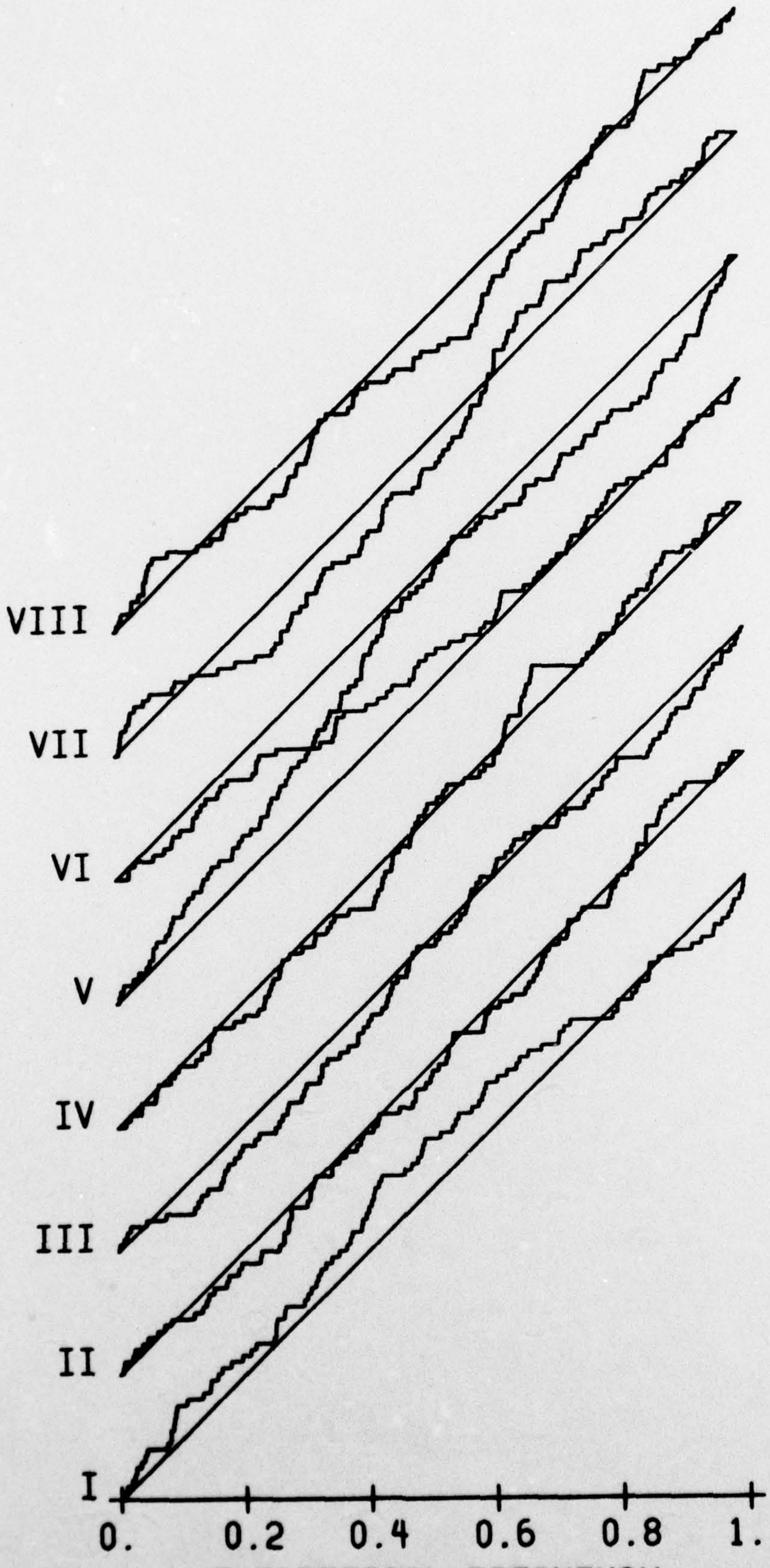


Figure 2. CHI-SQUARE TEST CDF

5. Serial Test Statistic

Hypothesis H_3 is designed to detect nonuniformity when the U_i are taken in nonoverlapping pairs or 2-tuples. One motivation for this testing arises from the theoretical observation in Marsaglia (1968) that the randomness of k-tuples becomes more suspect as k increases. The spectral and lattice tests support this observation. In particular, see Hoaglin (1976) and Marsaglia (1971). Ideally one would like to test for the uniformity in distribution of k-tuples over the k-dimensional unit hypercube. In practice, such testing is excessively expensive, even for $k = 2$.

Let us divide the unit interval into K cells, each of width $1/K$. Let N_{jk} denote the frequency with which V_i falls into the square $(((j-1)/K, j/K], ((k-1)/K, k/K])$. For fixed K the quantity

$$(3) \qquad S = \frac{K^2}{N} \Sigma_{j,k=1}^{K} (N_{jk} - N/K^2)^2$$

asymptotically has a chi-square distribution with $K^2 - 1$. Suppose we had chosen as before $K = 4096$. Then there would be $K^2 = 16777216$ cells. To guarantee a mean of 5 per cell under H_3 would require $N > 80$ million observations per replication or over 8 billion observations per multiplier. Since $2^{31} - 1 < 4.3$ billion such a sample size is not possible using this test procedure. Because of this demonstrated excessiveness we chose $K = 128$ which required 16384 cells, implied a cell width of 0.0078125 and, for $N = 200{,}000$, a mean of $n/K^2 = 12.21$ per cell under H_3. This choice of K enabled us to study the first 7 bits of the coordinates of V_i. Figure 3 shows the empirical cdf of S for each multiplier and column 3 of Table 1 gives the Kolmogorov-Smirnov statistics. Notice that no significance occurs, even for $\alpha = 0.20$.

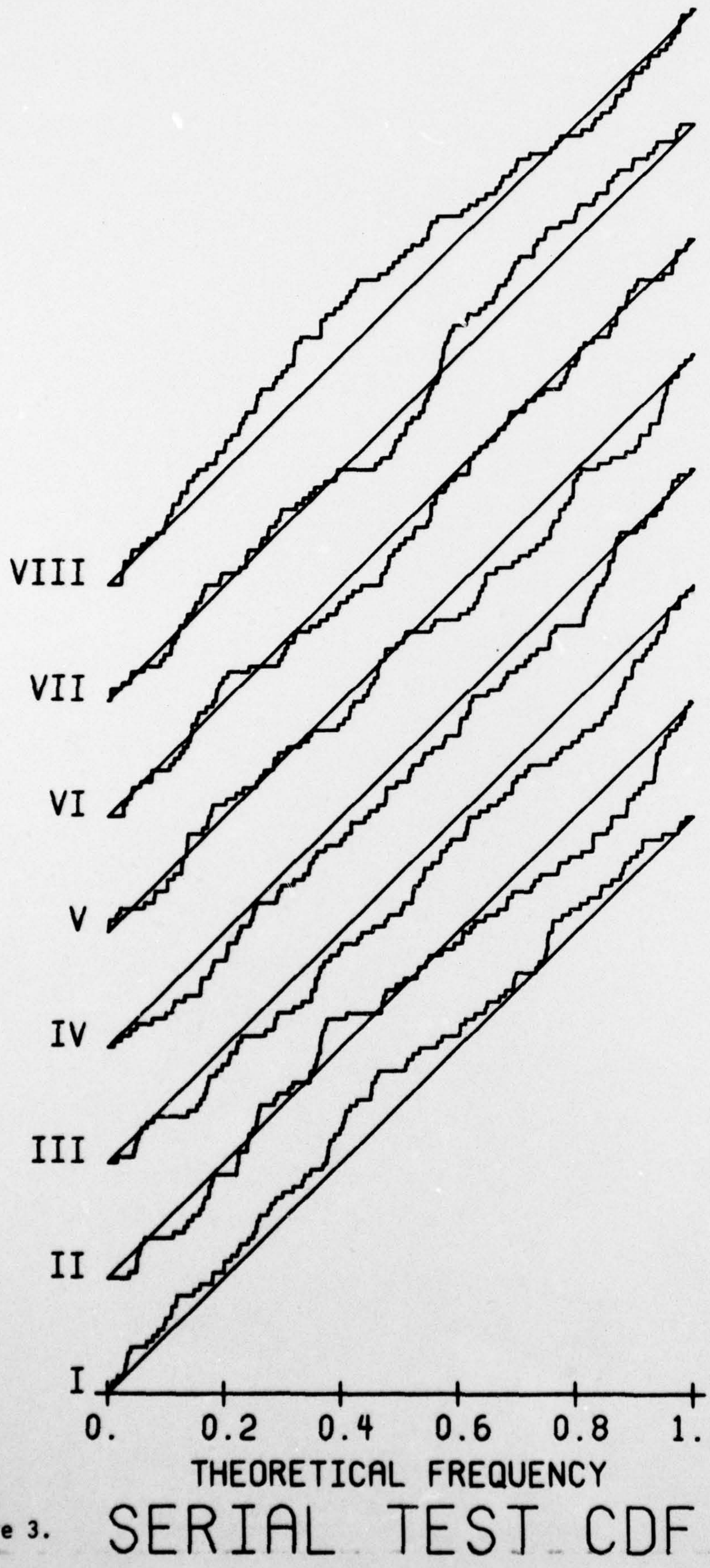

VIII
VII
VI
V
IV
III
II
I
0.
0.2
0.4
0.6
0.8
1.
THEORETICAL FREQUENCY
SERIAL TEST CDF

Figure 3.

6. An Additional K-S Type Statistic

Although the results in Table 1 raise moderate concern about multipliers III and VI only, the appearance of the empirical cdf's in Figures 1, 2 and 3 raises broader concern. Since the empirical cdf is a tied-down Brownian motion process [4], the properties of such a process may account for the drift apparent in many of the curves. As a further check on the empirical cdf's we studied an additional statistic for each empirical cdf:

$$X_n = \int_0^1 I_{[0,t]}(F_n(t))dt \quad .$$

This quantity denotes the proportion of $F_n(t)$ that falls below the 45 degree line. Using results in Dwass (1958) one can show that for given n X_n has the uniform distribution on $(0,1)$. Presumably, values of X_n close to 0 or 1 are suspect. Table 2 lists X_n in column 1 for the runs up and down, chi-square and serial test statistics for the 8 multipliers. Notice X_n raises suspicion about multipliers I, III and VI at the $\alpha = 0.05$ level and about IV and VII at the $\alpha = 0.20$ level. In particular, the results for X_n indicate that the empirical cdf's for multipliers I, III, IV, VI and VII spend either more (or less) time above (below) the 45 degree line than theory suggests.

7. Anderson-Darling Test

Although the supplementary statistic X_n appears more discriminating than the Kolmogorov-Smirnov statistic, it weighs deviations equally, regardless of where they occur in (0,1). In an effort to assign more weight to deviations in the tails of the distributions we subjected the 24 empirical cdf's to the

Table 2

Additional Test Results

Multiplier	X_n (1)	Y_n † (2)
Runs Up and Down		
I	0.2433	0.5208
II	.6811	.6278
III	.2924	1.4979**
IV	.7399	.6693
V	.5097	.4131
VI	.8406	.8298
VII	.0604**	1.3526
VIII	.7251	1.2748
Chi-Square		
I	.2092	1.4235**
II	.7110	.3326
III	.8204	.7583
IV	.5567	.3566
V	.1341	1.2414
VI	.9828*	1.5360**
VII	.5094	1.2628
VIII	.7165	.7647
Serial		
I	.0207*	.8981
II	.6969	1.2124
III	.9786*	1.2242
IV	.9372**	.8480
V	.7272	.8903
VI	.7318	.2931
VII	.2999	.7091
VIII	.2443	1.2357

*Significant for two tailed test at $\alpha = 0.05$ level.

**Significant for two tailed test at $\alpha = 0.20$ level.

†Significance points were computed for Y_n using Anderson and Darling's expression for the asymptotic distribution in [1].

Anderson-Darling test (1952, 1954). The test statistic is

$$Y_n = n \int_0^1 \{[F_n(t) - t]^2/t(1 - t)\}dt \quad .$$

Since $F_n(t)$ has mean t and variance $t(1 - t)/n$, Y_n is the integral of sample mean-square errors normalized by their theoretical mean-square errors. Anderson and Darling (1952) give the asymptotic distribution of Y_n and indicate that this limiting form is approached rapidly. Table 2 lists the Y_n and raises suspicion about multipliers I, III and VI at the $\alpha = 0.20$ level.

8. Execution Time

Although randomness considerations principally determine a multiplier's acceptability, efficiency in execution also plays a role. This is especially true when one regards several multipliers as equally good with regard to H_1, H_2 and H_3 and must decide which to use in practice. Column 4 of Table 1 lists relative execution times for the 8 multipliers, based on runs performed at the University of North Carolina Computation Center with interrupts due to other users eliminated. The wide disparity in execution times confirms a similar observation in Learmonth (1975). If one plots the multiplier value A against execution time, an approximate linear relationship appears. This may be due to the increasing number of modulo reductions that occur per multiplication as A increases.

9. Conclusions and Recommendations

Table 3 presents summary test results. They arouse serious suspicion about multipliers III and VI and suspicion about I, IV and VII. Therefore,

a conservative user would select multiplier II, V or VIII. Since II is in relatively common use, as in the simulation programming language SIMSCRIPT II, one may wish to rely on this choice. However, Table 1 clearly shows that V is the most efficient from the viewpoint of execution and statistical acceptance.

Table 3

Summary Test Results†

Multiplier	D_n	X_n	Y_n
I		S*	C*
II			
III	R**	S*	R**
IV		S**	
V			
VI	C**	C*	C**
VII		R**	
VIII			

†R ≡ runs statistic, C = chi-square statistic, S ≡ serial statistic;

A single asterisk denotes significance at $\alpha = 0.05$ and a double asterisk, significance at $\alpha = 0.20$.

10. References

1. Anderson, T. W. and D. A. Darling (1952). "Asymptotic Theory of Certain Goodness of Fit Criteria Based on Stochastic Processes", Ann. Math. Stat., Vol. 23, pp. 193-212.

2. Anderson, T. W. and D. A. Darling (1954). "A Test of Goodness of Fit", J. A. S. A., Vol. 49, pp. 765-769.

3. Coveyou, R. R. and R. D. MacPherson (1967). "Fourier Analysis of Uniform Random Number Generators", J. ACM, Vol. 14, pp. 100-119.

4. Durbin, J. (1973). Distribution Theory for Tests Based on the Sample Distribution Function, Society for Industrial and Applied Mathematics, Philadelphia, Pennsylvania.

5. Dwass, M. (1958). "On Several Statistics Related to Empirical Distribution Functions", Ann. Math. Stat. Vol, 29, pp. 188-191.

6. Hoaglin, D. (1976). "Theoretical Properties of Congruential Random-Number Generators: An Empirical View", Memorandum NS-340, Department of Statistics, Harvard University.

7. IBM, SIMPL/1 Program Reference Manual (1972). SH19-5060-0.

8. Jannson, Birger (1966). Random Number Generators, Almqvist and Wiksell, Stockholm.

9. Katzan, H., Jr. (1971). APL User's Guide, Van Nostrand Reinhold, New York.

10. Learmonth, G. P. (1975). "Empirical Tests of Multipliers for the Prime-Modulus Random Number Generator $X_{i+1} \equiv AX_i \text{ Mod } 2^{31} - 1$", Proceedings of the Ninth Interface Symposium on Computer Science and Statistics, D. C. Hoaglin and R. E. Welsch, eds. .

11. Learmonth, J. and P. A. W. Lewis (1973). "Naval Postgraduate School Random Number Generator Package LLRANDOM, Monterey.

12. Levene, H. and J. Wolfowitz (1944). "The Covariance Matrix of Runs Up and Down", Ann. Math. Stat., Vol. 15, pp. 58-66.

13. Lewis, P. A. W., A. S. Goodman and J. M. Miller (1969). "A Pseudo-Random Number Generator for the System/360", IBM Systems J., Vol. 8, No. 2, pp. 136-145.

14. Marsaglia, G. (1968). "Random Numbers Fall Mainly in the Planes", Proc. Natl. Acad. Sci., Vol. 61, pp. 25-28.

15. Marsaglia, G. (1972). "The Structure of Linear Congruential Sequences", in Applications of Number Theory to Numerical Analysis, S. K. Zaremba, ed., Academic Press.

16. Owen, D. H. (1962). Handbook of Statistical Tables, Addison-Wesley, Reading, Mass.

17. Payne, W. H., J. R. Rabung and T. P. Bogyo (1969). "Coding the Lehmer Pseudo-random Number Generator", Comm. ACM, Vol. 12, No. 2, pp. 85-86.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER 77-12	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Empirical Testing of Multiplicative Congruential Generators with Modulus $2^{31}-1$		5. TYPE OF REPORT & PERIOD COVERED Technical Report 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) George S. Fishman and Louis R. Moore		8. CONTRACT OR GRANT NUMBER(s) N00014-76-C-0302 ✓
9. PERFORMING ORGANIZATION NAME AND ADDRESS University of North Carolina Chapel Hill, N. C. 27514		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Operations Research Program Office of Naval Research Arlington, Virginia		12. REPORT DATE October 1977 13. NUMBER OF PAGES 15
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Distribution of this document is unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Anderson-Darling Test
Chi-Square Test
Kolmogorov-Smirnov Test
Multiplicative Congruential Generator
Random Number Generator
Runs Up and Down Test
Serial Test

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This paper presents the results of empirically testing 8 alternative multipliers for a multiplicative congruential generator with modulus $2^{31}-1$. The LLRANDOM random number package [11] uses one of the multipliers, the simulation programming language SIMSCRIPT II uses a second and the remaining six are the best of 50 candidate multipliers studied by Hoaglin (1976) using the theoretical spectral and lattice tests. The battery of tests fail to

detect any departures from randomness for 3 of the multipliers, even at a 0.20 significance level. This group includes the multiplier that SIMSCRIPT II employs. However, another of the 3 superior performers, 397204094, requires only 78 percent of the computing time that the SIMSCRIPT II multiplier does and is the second most efficient computationally of all 8 multipliers.